SECRET

IBSEC-CSS-R-4

MEMORANDUM FOR: Chairman, United States Intelligence Board
Security Committee

SUBJECT : Security Threat Analysis of Computer Operations

1. Reference is made to the 19 January 1970 tasking of the Computer Security Subcommittee to conduct an analysis of the security threat posed by the possibility of hostile exploitation of weak points in the computer operations of the Intelligence Community. In assigning this task to the Subcommittee, the Security Committee requested that the Counterintelligence Staff of CIA be asked to report any known cases where hostile services had attempted to exploit the security vulnerabilities of our computer operations; in addition the Subcommittee was asked to study the postulated threat of hostile penetration of our computer operations.

2. Inherent in any examination of hostile attempts to exploit our computer resources is the known Soviet Bloc interest in American computing technology. It is well recognized in the Community that the Soviet Union and its allies, being behind the United States in experimental construction, quantity production, and hardware/software design, has placed considerable effort and emphasis in its

SECRET

computer development programs to reduce or close the gap. The fact that the Soviet Union and its allies are involved in large scale overt efforts to collect information on Western computer technology is also well documented. It is also recognized that the Soviets are conducting covert operations to collect similar information regarding Western computer technology.

3. Examination of the problem by the Subcommittee has emphasized the possible exploitation of vulnerabilities in our computer operations by hostile agencies for the purpose of collecting information on American intelligence activities and USIB organizations.

4. As requested by the Security Committee, the Counterintelligence Staff of the Central Intelligence Agency was asked to examine their files for the purpose of identifying specific cases of known or suspected exploitation of Community computing operations. In addition, all Subcommittee members were asked to seek similar information from their separate agencies. While the results of this review in many cases were negative, the Central Intelligence Agency and the Federal Bureau of Investigation were able to provide information on several cases involving hostile attempts to exploit either personnel associated with Community computer operations or personnel employed by American computing manufacturers having potential contact with government operations.

Next 5 Page(s) In Document Exempt

Approved For Release 2004/02/10 : CIA-RDP79M00096A000100070006-3

9. Examples of criminal cases highlight the possibility that a hostile service could exploit the security vulnerabilities of our computer operations even though none of the agencies reported any evidence of such exploitation.

10. The second part of the task assigned to the Computer Security Subcommittee concerned the study of the postulated threat of hostile penetration of computer operations. This problem was previously addressed in a report prepared by the Defense Science Board Task Force on Computer Security. The final draft of this report was submitted in January 1970; however, the report has not yet been cleared for general release.

11. The Defense Science Board report notes that computer systems, by their nature, bring together a series of vulnerabilities which tend to jeopardize the system's information protection capabilities. Specific points of vulnerability can be classified into five groups:

a) Physical surroundings;

b) Hardware;

c) Software;

d) Communication links;

e) Personnel and organizational procedures.

12. The vulnerabilities postulated in the Defense Science Board report have been determined, at least in some cases, to be real. For example, CIA recently reported an incident where a programmer called for a dump of his memory partition in case of a fatal error. The error condition occurred and the resultant dump contained his program plus data from another user.

13. It was determined that the programmer had requested a specific core region size in accordance with the specification required of all programs run on the OS/MVT (multiprogramming) system. The program had not used the total region, thus the remaining core in the region had not been erased by the overlay of the program. However, the program abort reverted control to the operating system which dumped the total region, including the non-erased core, from the previous user rather than just the selective area occupied by the program.

14. The system was modified so that the terminator routine (controlled by OS) erases all core in a region upon termination of a job. However, the fact remains that the vulnerability did exist undetected within the system for a period of time prior to discovery.

15. AEC reported an incident regarding a technique which could permit the accidental or intentional disclosure of classified data or information to unauthorized personnel through bypassing the storage protection feature of main memory. This deficiency was accidentally detected while checking out a scientific computer program on an IBM 360/50 using OS/MVT (Operating System 360 which does multiprogramming with a variable number of tasks) Version 18.

Discussion with IBM revealed that all IBM 360 computer systems operating under the control of Disk Operating System (DOS), Tape Operating System (TOS), Basic Operating System, Basic Programming System (BPS) and Operating System (OS/360) are vulnerable to this technique. This deficiency can be corrected by the fetch protection feature offered by IBM; however, fetch protection can be installed only on IBM models 360/50 and above.

16. Deliberate attempts mounted against a system to take advantage of or create weak points would usually require a combination of a system design shortcoming either unforeseen or undected and placement of someone in a position to initiate action. The fact that there is no present evidence of hostile attempts to technically penetrate Community computer systems should not preclude USIB member agencies from seriously considering the postulated threat and should not cause these agencies to relax preventative measures against the actual threat.